IN THE DRAWINGS

The attached sheets of drawings include changes to Figs. 3, 4 and 6. These sheets,

which include Figs. 3, 4 and 6, replace the original sheets including Figs. 3, 4 and 6.

Attachment: Replacement Sheets (3)

REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1, 4, 6, 7, 9 and 14-39 are pending in the present application. Claims 2, 3, 5, 8 and 10-13 are canceled, Claims 1, 4, 6, 7, 9 are amended, and Claims 14-39 are added by the present amendment. In addition, the specification and Figures 3, 4 and 6 are amended·

Amendments to the claims finds support in the specification as originally filed at least at Figures 1-6 and page 4, line 15, to page 7, line 21. Further, the specification and Figures 3, 4 and 6 are amended to correct minor inconsistencies. Thus, it is believed no new matter is added.

In the outstanding Office Action, Claim 1 was rejected under 35 U.S.C. § 112, second paragraph and Claims 1-13 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,751,805 to Otsuki et al. (herein "Otsuki").

Regarding the rejection of Claim 1, under 35 U.S.C. § 112, second paragraph, Claim 1 is amended to more clearly recite the claimed subject matter in light of comments in the outstanding Office Action. Accordingly, it is respectfully requested that rejection be withdrawn.

Applicants respectfully traverse the rejection of Claims 1-13 under 35 U.S.C. § 102(b) as anticipated by Otsuki with respect to amended independent Claims 1, 4 and 7 and new independent Claims 24, 31 and 37.

Amended independent Claim 1 is directed to an encryption algorithm management system that includes a terminal unit and a center unit each having a common cipher-key. The terminal unit includes, *inter alia*, an encryption controller configured to renew the common cipher-key in case of receiving encrypted data from the center unit and to decrypt an encryption algorithm from a ciphered encryption algorithm. Amended independent Claim 4

13

and independent Claim 31 are directed to a terminal unit including similar features and independent Claim 24 is directed to a system having a terminal unit including similar features.

Amended independent Claim 1 is further directed to a center unit including, *inter alia*, a key controller configured to renew the common cipher-key to be identical with the renewed common cipher-key in the terminal unit and an encoder configured to produce encrypted data by encrypting a cipher-key for a ciphered encryption algorithm with the renewed common cipher-key and transmit the encrypted data to the terminal unit. Amended independent Claim 7 is directed to a center unit including similar features.

Independent Claim 24 is directed to a system having a center unit including, *inter alia*, a key controller configured to renew the common cipher-key to be identical with the renewed common cipher-key in the terminal unit and an encoder configured to produce a ciphered encryption algorithm with the renewed common cipher-key. Independent Claim 37 is directed to a center unit including similar features.

In a non-limiting example, Applicants' Figures 1 and 2 show an encryption algorithm management system including a center unit and a terminal unit that share a common cipher-key Kt. The terminal unit 20i in this example includes an encryption algorithm controller 23 (e.g., encryption controller) that decrypts an encryption algorithm Al from ciphered encryption algorithm E2(KAl)[Al]. The decrypted encryption algorithm Al is used by an encryption and decryption controller 24 to encrypt a message M sent to another terminal unit. The center unit 10 in this example includes an encoder 14 that encrypts a cipher-key KAl for a ciphered encryption algorithm E2(KAl)[Al] with the renewed common cipher-key Kt, and transmits the encrypted data E1(Kt)[KAl] to the terminal unit. A controller 11 in the center unit 10 inputs a state value t into a stream cipher 12, which produces a renewed common cipher-key Kt based on the state value t each time a renewed cipher-key is required (e.g.,

upon demand or when encrypted data is received). The same state value t is also stored in the terminal unit 20i.

In this example, the user goes to the center for a cipher-key and the cipher-key that is sent form the center changes each time. In particular, t (the state value) of [Kt] changes. In other words, on the first occasion, it is K1, on the second occasion it is K2, etc...

In other words, Figures 1 and 2 show an example of an embodiment of the present invention in which it is necessary to obtain encryption data from a center unit 10 when the encryption algorithm decryption cipher-key is updated. Thus, the encryption algorithm that is employed in the encryption algorithm using system can be managed and dishonest use of the encryption algorithm can be prevented. The encryption algorithm controller 23 is in a memory region that is incapable of being rewritten from outside the terminal (e.g., PC, etc...) and whose contents cannot be read. Therefore, making it possible to prevent tampering by a malicious third party. The controller 11 checks for the existence of the right to use the encryption algorithm by the terminal unit 20i. Then, if the right to use exists, updating the state value t in the stream cipher 12 thereby providing management of the encryption algorithm.

In addition, the non-limiting embodiment of Figures 3 and 4 shows a similar system. However, in the embodiment of Figures 3 and 4, encryption data of the encryption algorithm (e.g., encrypted data E2(Kt)(Al)) is sent by the center unit 10a instead of the encryption data of the decryption cipher-key. At the terminal unit 20ia a request is sent to the center unit 10 on every nth use of the encryption algorithm. A counter 32 is included in the encryption algorithm management unit 30. The encryption algorithm management unit 30 is in a memory region that cannot be rewritten from outside the terminal (e.g., PC, etc...) and whose contents cannot be read, thereby making it possible to prevent tampering by a malicious third party, as in the embodiment of Figures 1 and 2.

In other words, encrypted data E2(Kt)(Al) is used with cipher-key Kt to produce Al (decryption result), but decrypting encrypted data E2(kt)[Al] with cipher-key Kt+1 produces random data as the decryption result when the counter 32 indicates n or more. Further, the algorithm to be encrypted Al and cipher-key Kij are used to produce encrypted data E(Al, Kij)[M] from message M, in general.

In addition, the non-limiting embodiment of Figures 5 and 6 shows a similar system. However in the embodiment of Figures 5 and 6, the terminal unit makes a decryption request to the center unit 10 on each occasion that the decryption cipher-key has been used n times. The cipher-key information memory 21b, cipher-key information management unit 40, first cipher-key decryption controller 42, and second cipher-key decryption controller 45 are newly provided. The encrypted data E1(ki)[Kij] of the cipher-key Kij and the encrypted data E1(kt)[KAl] of the decryption cipher-key are memorized. Hence, when the counter 43 indicates n or more, random data is the decryption result. Accordingly, dishonest use of the encryption algorithm is prevented by management of the encryption algorithm used in the encryption algorithm system.

Accordingly, the user must receive the data (message) together with the decryption cipher-key sent to the user from the center. Thus, dishonest use by an imposter user, who does not have the decryption cipher-key, can therefore of course not be performed. Further, a surcharge can be required even if a genuine user performs use more than a prescribed number of times (e.g., necessary number of times). Thus, this arrangement advantageously allows management of encryption algorithms and prevention of unauthorized use of encryption algorithms by periodically renewing a common cipher-key in both terminal unit and center unit and sending either a cipher-key for the encryption algorithm or a ciphered encryption algorithm to the terminal unit from the center unit.[1]

---

[1] Specification at page 10, line 5, to page 11, line 9.

16

Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest an encryption algorithm management system including a terminal unit and a center unit that renew a common cipher-key when receiving encrypted data at the terminal unit or when receiving a demand at the center unit. <u>Otsuki</u> describes a data-protecting system that includes a software supplier (e.g., center unit) that encrypts a program P with a random number K to produce an encrypted program P'.[2] Further, in <u>Otsuki</u> the software supplier encrypts the random number K using an encryption key Kpu (e.g., common cipher-key) to produce an encrypted key K',[3] and sends the encrypted key K' and encrypted program P' to the user (e.g., terminal unit).[4] In <u>Otsuki</u>, the user decrypts the encrypted key K' using another encryption key Kup (e.g., common cipher-key) and decrypts the encrypted program P' based on K.[5] <u>Otsuki</u> does not describe how the encryption key Kpu is generated, but only shows that in Figs. 2 and 3 Kpu appears to be a function of a program password PIN-P and user identifier IDu. Further, <u>Otsuki</u> indicates that encryption key Kup is arithmetically obtained by a loader based on the secret algorithm and the identifier of the user or program,[6] but is silent regarding any way to renew encryption keys Kup and Kpu. Further, <u>Otsuki</u> is silent regarding any means for the user to demand that encrypted data be received from the software supplier (e.g., center unit).

Hence, Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest a terminal unit or an encryption algorithm management system that includes a terminal and a center unit "having a common cipher-key," and the terminal unit including a transmitter "configured to transmit a demand to said center unit for obtaining an encrypted data," and an encryption controller "configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand," as recited in independent Claims 1, 4, 24 and 31.

---

[2] <u>Otsuki</u> at column 5, lines 3-9.
[3] <u>Otsuki</u> at Figs. 2 and 3, and at column 5, lines 22-25, and column 6, lines 48-51.
[4] <u>Otsuki</u> at column 5, lines 37-38.
[5] <u>Otsuki</u> at column 4, lines 5-10 and lines 41-44.
[6] <u>Otsuki</u> at column 6, lines 38-40.

Similarly, Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest a center unit or an encryption algorithm management system that includes a center unit having a key controller "configured to renew said common cipher-key so as to be identical with said renewed common cipher-key in case of receiving said demand from said transmitter," as recited in independent Claims 1, 7, 24 and 37.

Further, Applicants note that <u>Otsuki</u> describes a system that allows a user to perform decryption any number of times, once the user has received the code. For example, in <u>Otsuki</u> once a user has received the encrypted authorization number from a video shop, the user can rent a video cassette or DVD any number of times using this encrypted authorization number (so-called rental video shop algorithm). Hence, for this reason as well as the reasons above, <u>Otsuki</u> does not teach or suggest an encryption controller "configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand," as recited in independent Claims 1, 4, 24 and 31.

Accordingly, Applicants respectfully submit independent Claims 1, 4, 7, 24, 31 and 37, and claims depending therefrom, are allowable at least for the reasons discussed above.

In addition, Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest a terminal unit, or an encryption algorithm management system including a terminal unit, that includes an encryption controller configured to decrypt an encryption algorithm from a ciphered encryption algorithm and to send a message using the encryption algorithm to another terminal. As discussed above, <u>Otsuki</u> merely indicates that a user decrypts a program P from an enciphered program P', but is silent regarding a program P that includes an encryption algorithm and is silent regarding a terminal unit that uses the decrypted encryption algorithm to send a message. Further, <u>Otsuki</u> indicates that it is desirable for the decryption algorithm in the ACE (e.g., carrier unit in the user) to be capable of being upgraded.

18

However, <u>Otsuki</u> does not provide any description or example of a method or apparatus for upgrading the decryption algorithm of the user.[7]

Hence, Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest a terminal unit configured to "decrypt a cipher-key for the ciphered encryption algorithm [and] decrypt an encryption algorithm from the ciphered encryption algorithm" as recited in independent Claims 1, 4, 24 and 31, and "encrypt a message with the encryption algorithm and send the encrypted message to a second terminal," as recited in Claims 15, 21, 26 and 33.

Further, Applicants respectfully submit that <u>Otsuki</u> also does not teach or suggest the features of new Claim 39.

Claim 39 is directed to an encryption algorithm management system with a terminal unit that includes, *inter alia*, an encryption controller that has a counter for counting a number transmitted from a controller. If the counter receives a number transmitted from the controller more than a prescribed number of times, the encryption controller does not produce an encryption algorithm by decrypting the encrypted data with a renewed common cipher-key. Thus, with this arrangement the encrypted algorithm cannot be converted if the encrypted cipher-key has been used more than a presecribed number of times. For example, counter 32/41 is used to set the allowed number of times of use (n).

Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest a counter or an encryption controller having such a function. Conversely, in <u>Otsuki</u>, a first encrypted cipher-key and a second, further encrypted cipher-key using the first encrypted cipher-key are necessary, and a loader is required for decryption. Further, for decryption <u>Otsuki</u> also requires a first encrypted cipher-key and a second further encrypted cipher-key using the first encrypted cipher-key. Hence, Applicants respectfully submit that <u>Otsuki</u> does not teach or suggest an encryption controller that "has a counter for counting a number transmitted from a

---

[7] <u>Otsuki</u> at column 4, lines 47-50.

19

controller, and if said counter receives a number transmitted from said controller more than a

prescribed number of times, said encryption controller does not produce an encryption

algorithm by decrypting said encrypted data with said renewed common cipher-key," as

recited in new Claim 39.

Accordingly, Applicants respectfully submit independent Claims 1, 4, 7, 24, 31, 37

and 39, and claims depending therefrom, are allowable at least for the reasons discussed

above.

Consequently, in light of the above discussion and in view of the present amendment,

the present application is believed to be in condition for allowance and an early and favorable

action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK:ZSS:dnf

I:\ATTY\ZS\19's\198274US\198274US-AM.030105.DOC